Y 4. G74/7:Se 2/8

SECURITY WEAKNESSES IN TREASURY'S FINANCIAL DISBURSEMENT SYSTEMS

COMPLETED
44

HEARING

BEFORE A

SUBCOMMITTEE OF THE

COMMITTEE ON GOVERNMENT OPERATIONS HOUSE OF REPRESENTATIVES

NINETY-NINTH CONGRESS

SECOND SESSION

MARCH 11, 1986

Printed for the use of the Committee on Government Operations

ORIGINAL

U.S. GOVERNMENT PRINTING OFFICE
59-122 O WASHINGTON : 1986

COMMITTEE ON GOVERNMENT OPERATIONS

JACK BROOKS, Texas, *Chairman*

DON FUQUA, Florida
JOHN CONYERS, Jr., Michigan
CARDISS COLLINS, Illinois
GLENN ENGLISH, Oklahoma
HENRY A. WAXMAN, California
TED WEISS, New York
MIKE SYNAR, Oklahoma
STEPHEN L. NEAL, North Carolina
DOUG BARNARD, Jr., Georgia
BARNEY FRANK, Massachusetts
TOM LANTOS, California
ROBERT E. WISE, Jr., West Virginia
BARBARA BOXER, California
SANDER M. LEVIN, Michigan
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
JOHN M. SPRATT, Jr., South Carolina
JOE KOLTER, Pennsylvania
BEN ERDREICH, Alabama
GERALD D. KLECZKA, Wisconsin
ALBERT G. BUSTAMANTE, Texas
MATTHEW G. MARTINEZ, California

FRANK HORTON, New York
THOMAS N. KINDNESS, Ohio
ROBERT S. WALKER, Pennsylvania
WILLIAM F. CLINGER, Jr., Pennsylvania
ALFRED A. (AL) McCANDLESS, California
LARRY E. CRAIG, Idaho
HOWARD C. NIELSON, Utah
JIM SAXTON, New Jersey
PATRICK L. SWINDALL, Georgia
THOMAS D. (TOM) DeLAY, Texas
JOSEPH J. DioGUARDI, New York
RICHARD K. ARMEY, Texas
JIM LIGHTFOOT, Iowa
JOHN R. MILLER, Washington
BEAU BOULTER, Texas
JOHN E. GROTBERG, Illinois

WILLIAM M. JONES, *General Counsel*
STEPHEN M. DANIELS, *Minority Staff Director and Counsel*

COMMERCE, CONSUMER, AND MONETARY AFFAIRS SUBCOMMITTEE

DOUG BARNARD, Jr., Georgia, *Chairman*

JOHN M. SPRATT, Jr., South Carolina
JOE KOLTER, Pennsylvania
BEN ERDREICH, Alabama
ALBERT G. BUSTAMANTE, Texas

LARRY E. CRAIG, Idaho
PATRICK L. SWINDALL, Georgia
JIM SAXTON, New Jersey

EX OFFICIO

JACK BROOKS, Texas

FRANK HORTON, New York

PETER S. BARASH, *Staff Director*
THEODORE J. JACOBS, *Chief Counsel*
DONALD P. TUCKER, *Chief Economist*
STEPHEN R. McSPADDEN, *Counsel*

For sale by the Superintendent of Documents, Congressional Sales Office
U.S. Government Printing Office, Washington, DC 20402

CONTENTS

Page

Hearing held on March 11, 1986 1

Statement of:

Barnard, Hon. Doug, Jr., a Representative in Congress from the State of Georgia, and chairman, Commerce, Consumer, and Monetary Affairs Subcommittee: Opening statement 1

Douglas, William E., Commissioner, Financial Management Service, Department of the Treasury, accompanied by Marcus Page, Deputy Commissioner 19

Hill, Michael R., acting inspector general, Department of the Treasury, accompanied by Robert P. Cesca, assistant inspector general for Fiscal Services and ADP, and Maurice S. Moody, Director of Audit, Financial Management Service 12

Simonette, John F., Associate Director, Accounting and Financial Management Division, General Accounting Office, accompanied by Chris Martin, auditor, and James K. Krawchyk, group director 2

Letters, statements, etc., submitted for the record by:

Douglas, William E., Commissioner, Financial Management Service, Department of the Treasury:

Electronic certification, estimated implementation costs 22

Historical background, electronic certification, Financial Management Service 21

Hill, Michael R., acting inspector general, Department of the Treasury:

Authentication program of former Treasury Secretary Regan 19

Data concerning electronic transfer of Treasury funds offshore 17

Information concerning $800,000 theft 15

Speed and adequacy of the reconciliation process 16

Simonette, John F., Associate Director, Accounting and Financial Management Division, General Accounting Office:

Transferring funds offshore using Fedwire 9-10

Treasury financial communications system 5

Treasury reported payment volumes, fiscal year 1985 3

APPENDIXES

Appendix 1.—Responses by John F. Simonette, Associate Director, Accounting and Financial Management Division, General Accounting Office, to additional questions submitted by the subcommittee 27

Appendix 2.—Responses by Michael R. Hill, acting inspector general, Department of the Treasury, to additional questions submitted by the subcommittee 34

Appendix 3.—Responses by William E. Douglas, Commissioner, Financial Management Service, Department of the Treasury, to additional questions submitted by the subcommittee 38

SECURITY WEAKNESSES IN TREASURY'S FINANCIAL DISBURSEMENT SYSTEMS

TUESDAY, MARCH 11, 1986

HOUSE OF REPRESENTATIVES,
COMMERCE, CONSUMER, AND
MONETARY AFFAIRS SUBCOMMITTEE
OF THE COMMITTEE ON GOVERNMENT OPERATIONS,
Washington, DC.

The subcommittee met, pursuant to call, at 10 a.m., in room 2203, Rayburn House Office Building, Hon. Doug Barnard, Jr. (chairman of the subcommittee) presiding.

Present: Representative Doug Barnard, Jr.

Also present: Peter S. Barash, staff director; Faye Ballard, clerk; Scott Fisher, minority professional staff, Committee on Government Operations, and Mike Eid, GAO employee detailed to the subcommittee.

OPENING STATEMENT OF CHAIRMAN BARNARD

Mr. BARNARD. The subcommittee will come to order.

Today the Commerce, Consumer, and Monetary Affairs Subcommittee will examine security weaknesses in the financial disbursement systems at the Department of the Treasury.

Each year, these systems process hundreds of millions of payments representing hundreds of billions of dollars. Virtually every American is affected in one way or another by these payments. Medicare, Social Security, veterans' benefits, bills for goods and services sold to the Government, aid to State and local governments, and Federal employees' salaries are all paid through Treasury's disbursement systems.

The subcommittee has possession of reports prepared by the General Accounting Office, the Treasury Department's inspector general, and consultant reports commissioned by Treasury, which conclude that the disbursement systems are dangerously vulnerable to fraud and abuse. In fact, we will hear testimony today that these systems have already been the target of a number of fraudulent schemes, some resulting in substantial losses.

The purpose of today's hearing is to examine the nature and extent of these thefts, identify what weaknesses exist and what can be done to correct them, and assess the adequacy of Treasury's efforts to protect the integrity of the Department's disbursement systems.

A crucial factor we need to consider is that the Treasury's financial communications system, known as TFCS, is an electronic

system that transfers billions of dollars, almost instantaneously, through the Fedwire or private wire transfer services, into payee accounts throughout the country and even throughout the world, including accounts in tax haven and bank secrecy jurisdictions. While the margin for error in making fraudulent payments is apparently great, the reaction time available to discover and correct such payments is extremely small. It is vitally important, therefore, that every measure possible be taken now, before the fact, to assure the security of these systems.

Some of the specifics of today's testimony are extremely sensitive. If the wrong people were to learn the details of the systems' vulnerabilities, the Government's payments would be placed in even greater jeopardy. Consequently, after we have heard from all the witnesses, the subcommittee will possibly go into executive session.

In addition, I would advise the witnesses that if you believe a question should not be answered in open session because of a threat to the security of the disbursement systems, you should feel free to ask that the response be deferred to executive session.

Our first witness this morning is Mr. John Simonette of the General Accounting Office. He will be accompanied by Mr. Chris Martin and Mr. James K. Krawchyk.

Would you gentlemen please take the witness table?

Mr. Simonette, you might want to further introduce your two associates this morning. I want to welcome you to the hearing this morning and likewise commend you and your staff on this study that you have made and for appearing here today to go over it with us.

I'll now turn the microphone over to Mr. John Simonette.

STATEMENT OF JOHN F. SIMONETTE, ASSOCIATE DIRECTOR, ACCOUNTING AND FINANCIAL MANAGEMENT DIVISION, GENERAL ACCOUNTING OFFICE, ACCOMPANIED BY CHRIS MARTIN, AUDITOR, AND JAMES K. KRAWCHYK, GROUP DIRECTOR

Mr. SIMONETTE. Thank you very much, Mr. Chairman. We appreciate the opportunity to appear today to discuss our review of the Treasury's financial communications system, generally referred to as TFCS.

Jim Krawchyk on my right is the group director and was responsible for the overall direction of this particular review. At my left at the easel is Chris Martin who was the auditor in charge of the review.

Although Treasury has been responsive to our recommendations to strengthen the system, some fundamental problems remain which affect other disbursement systems as well and leave the Government vulnerable to unauthorized payments. Hopefully, the dialog generated through this hearing will add impetus to the correction of these problems. Based on our findings and the billions of dollars the Government disburses, corrective action is clearly warranted.

Before I describe the nature of our review and findings, I would like to take a few moments to discuss Treasury's role as a paying agent. Treasury issues payments, electronically as well as through

checks, on behalf of most Government entities. Treasury operates seven financial centers around the country which receive and process agency payment requests. After verifying that the requests are properly authorized and provide all of the necessary information, such as the payee, amount, and the agency identification code, Treasury issues the payments.

Chart A shows Treasury's fiscal year 1985 reported payment volumes. As you can see, Treasury uses two methods for issuing payments electronically—direct deposit electronic funds transfer and, second, TFCS.

[Chart A follows:]

CHART A

TREASURY
REPORTED PAYMENT VOLUMES
FISCAL YEAR 1985

Method of Payment	Number of Payments
Checks	487.3 million
Direct Deposit/ Electronic Funds Transfer	233.2 million
TFCS	258 thousand

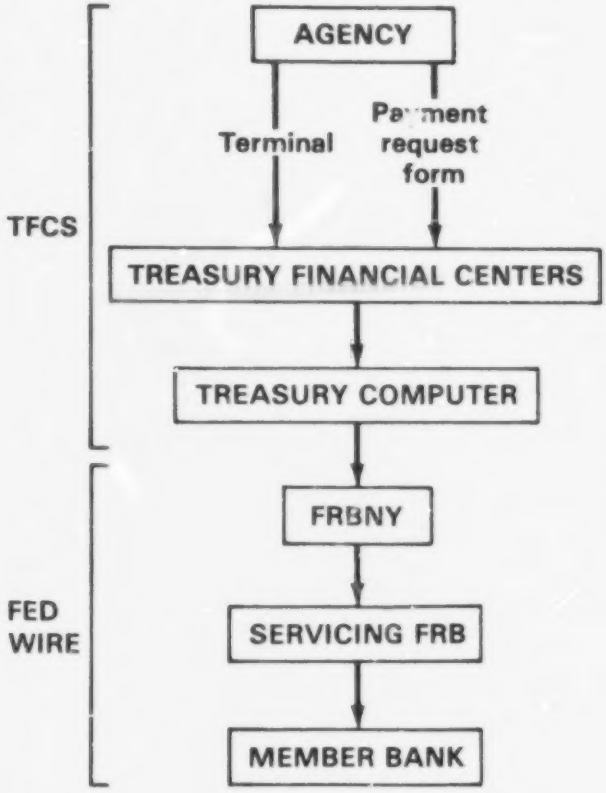
Mr. SIMONETTE. In the direct deposit method, Treasury assembles information on the payees' bank account numbers and payment amounts. This information is distributed to Federal Reserve banks and their branches and is then transmitted to the payees' financial institutions. Treasury uses this method where possible for high-volume, low-dollar recurring payments such as salary and Social Security benefits.

TFCS, on the other hand, is generally used for large, nonrecurring payments, such as letter of credit payments to Federal grant recipients and payments of $25,000 or more to vendors serving Federal agencies. TFCS differs from the direct deposit program in that it provides a computer-to-computer link to the Federal Reserve System for all its payments, as shown on chart B. This affords Treasury the capability to better control the scheduling and timing of disbursements.

[Chart B follows:]

CHART B

TREASURY FINANCIAL COMMUNICATIONS SYSTEM



Mr. SIMONETTE. At the time our review began, only two of the three Treasury financial centers now tied into TFCS were operational. As the chart shows, some agencies also were authorized to directly input payment data using terminals located in their offices. The payment volume has steadily increased, with transactions growing from $102 billion in fiscal year 1982 to $300 billion in fiscal year 1985.

Because of the increasing volume of payments being made through the system, we reviewed key aspects of TFCS as part of our ongoing efforts to evaluate agencies' internal controls. Our primary objective was to determine whether TFCS had adequate controls to ensure that only properly authorized payments were made. Based on our work, we concluded that the controls were inadequate to prevent unauthorized payments from being made or to ensure proper accounting for all payments. For example, it is essential that access to a system such as TFCS be adequately controlled. However, we found that because of a breakdown in system access controls it was possible for unauthorized Treasury personnel to make improper payments at one of the two Treasury financial centers we examined. We also noted that Treasury lacked adequate controls to ensure that a similar breakdown would not occur in other TFCS locations tied into the system.

Among the other problems we found were a lack of controls for preventing duplicate payments. We reviewed certain payments made at one Treasury financial center from August 1983 through January 1984. Treasury records identified six duplicate payments while we identified a seventh. These duplicate payments totaled about $5.4 million. Although the duplicate payments identified represented a very small portion of the 27,600 payments processed during that period, we could not verify that these were the only ones that occurred.

We also noted weaknesses in Treasury's procedures for ensuring the accuracy of payment information. This created the opportunity for erroneous data to be entered into the system which could have prevented or delayed processing of a properly authorized payment or allowed a fraudulent payment to be issued and its subsequent detection delayed. This particular weakness was magnified by the lack of control over agencies' payment requests which were vulnerable to manipulation by Treasury financial center personnel.

Some of the weaknesses we found in examining TFCS extended to payments made by checks and direct deposit electronic funds transfers, thus increasing the possibility of fraud. Although Treasury operates the disbursing systems, the other agencies serviced by Treasury share the responsibility of preventing unauthorized payments. However, our past audit work has shown that control breakdowns occur in the other agencies as well. Of course this increases our concern over the risk of fraudulent payments.

Given this type of environment, the obvious questions arise as to the magnitude of past losses and what must be done to better prevent fraud. Although it would not be appropriate to address these questions publicly at this time, I can offer some examples of what has happened. In one agency, an employee was able to embezzle over $555,000. The agency official was not apprehended until another employee noticed discrepancies in the records. In a different

agency, an employee embezzled more than $856,000 but called attention to himself by adopting an extravagant lifestyle. In yet another case, an agency recorded over $1 million of payments without establishing what the payments were for. This was done simply to bring the agency's records in line with Treasury's, and the agency didn't verify that the payments were for authorized purposes. These are all examples of breakdowns in agencies' controls.

Returning now to TFCS specifically, I would like to point out that Treasury had many controls already in the system when we began our review and that we know of no losses sustained by TFCS. However, because of the problems I've described, as well as others, we made several recommendations for improvements. In responding to our report, Treasury agreed with virtually all of our recommendations and stated that it had taken or would take corrective action. For example, Treasury implemented new controls to reduce the possibility of unauthorized individuals gaining access to the system. Treasury also reported that it was establishing new procedures for ensuring the accuracy of payment data entered into the system and for preventing duplicate payments. Treasury also has been working to correct the weaknesses that remain. On the whole, we are very encouraged by Treasury's response, which I understand will be described in more detail by Treasury today.

Mr. Chairman, that concludes my prepared statement for this portion of the hearing. As you know, we did not make our report available for public distribution because of the sensitivity of some of the issues that were covered. My remarks about TFCS thus far have pertained to matters which Treasury has adequately addressed. We will later present our views on the remaining problems and on what must be done to further reduce the Government's vulnerability to unauthorized payments. However, my staff and I will be glad to discuss any other questions that you may have at this time.

Mr. BARNARD. Thank you, Mr. Simonette.

Mr. Simonette, this question possibly will be answered at a later time, but has GAO been able to document all of the actual losses that have occurred through the system?

Mr. SIMONETTE. No, sir; we have not been able to document total actual losses. As far as we know, no such Government-wide data is available. There are several parties that become involved when fraudulent or potentially fraudulent activities occur. For example, the Secret Service is heavily involved in such cases, the FBI, and of course in some cases the agencies' inspectors general can be involved.

There is no central point at this time to collect such data, and we have not had the opportunity ourselves to contact each of these establishments to determine what information they may have.

Mr. BARNARD. In other words, you didn't follow through on the two cases that you enumerated when one employee embezzled over $555,000 and another one $856,000?

Mr. SIMONETTE. That's correct. We did not follow those through.

Mr. BARNARD. So you don't know whether or not there has been recovery of those sums.

Mr. SIMONETTE. There has been some recovery in at least one of those cases, I believe.

Mr. BARNARD. Mr. Simonette, the GAO's audit concluded that controls were inadequate to prevent unauthorized Treasury payments and to ensure proper accounting for all payments. You have testified this morning that fundamental problems remain which leave the Government vulnerable to unauthorized payments and that corrective action is clearly warranted.

Please tell the subcommittee exactly how concerned you are and how vulnerable the system is.

Mr. SIMONETTE. Mr. Chairman, we remain very concerned about the vulnerability of the system, as acknowledged in our statement. Treasury has been responsive to our report and has taken a number of actions. However, we are still concerned about the overall vulnerability, especially in terms of the input that is entered into that system, and, as we will discuss in an executive session, there are additional actions that are needed to ensure the authenticity of payment requests.

Mr. BARNARD. Mr. Simonette, given what you know about the check payment frauds that were committed, is there any reason to believe that they couldn't have been committed just as easily against the TFCS?

Mr. SIMONETTE. We believe that the same type of fraud could be committed through the TFCS. Basically, the overall payment process is the same, whether it's TFCS, check, or the electronic funds transfer.

Mr. BARNARD. But the payee on the TFCS is primarily what—cities and large—they are the large items. Wouldn't it be difficult to commit fraud in those areas, or would it?

Mr. SIMONETTE. Let me ask Mr. Martin to help respond to that, Mr. Chairman.

Mr. MARTIN. The payee on a TFCS payment can be an individual, corporation, a State, local government, anyone who has a bank account.

Mr. BARNARD. But they are the large ticket items, aren't they?

Mr. MARTIN. Correct.

Mr. BARNARD. $25,000 or more.

Mr. MARTIN. Correct. But it can still go to an individual.

Mr. BARNARD. Given the vulnerabilities in the present payment system, it seems to me that in terms of detecting fraud a great deal is riding on the speed and adequacy by which authorizations for payments are reconciled with the payments themselves. How much faith do you have in the speed and adequacy of the reconciliation process?

Mr. SIMONETTE. Mr. Chairman, we have seen problems in the reconciliation process. In some cases the reconciliation process was simply not getting performed at the agencies. So that's one problem—the reconciliation doesn't take place in some cases even though there is a Treasury requirement.

But reconciliation, while useful, is a detective control as opposed to a preventive control. In other words, it's a control that takes place after the transaction has been completed. If fraud has occurred and the payment has been made, then there is a need to try to recover the money.

So what we continue to emphasize is, while reconciliation has an important part in an overall payment process, the need is for up-

front preventive controls. We feel that in a payment process or any other control system the preventive controls are the more effective controls.

Mr. BARNARD. For laymen such as myself, reconciliation means balancing. Do you mean to tell me these books are not balanced periodically?

Mr. SIMONETTE. In some cases that occurs; yes, sir, Mr. Chairman.

Mr. KRAWCHYK. If I could just add to that, Mr. Chairman, there are really two levels of balancing for reconciliation to occur. There is a daily balancing between Treasury and the Federal Reserve Bank in New York. Secondarily to that, the agencies themselves must reconcile, at least on a monthly basis, their disbursement for each month, both what they have reported versus what Treasury reports to them that they have disbursed for the agency. It is in the agencies where we have seen the problem, a lack of timely reconciliation.

Mr. BARNARD. Is that because they have an open-ended overdraft?

Mr. KRAWCHYK. I wouldn't call it that so much as the way in which the Treasury systems work. The agencies may have some additional time to try to identify and record payments, even though there may be a discrepancy between their record and Treasury's.

Mr. BARNARD. Even if the reconciliation process was highly reliable, given the speed with which the sums are instantly transferred electronically throughout the country and the world, is it feasible to rely on the reconciliation process to prevent the theft of large sums of money?

Mr. SIMONETTE. It's not a completely reliable control, Mr. Chairman, because, again, it's a detective or a back-end type of control, and the question still remains as to the authenticity of the input that is going into the payment process—that is, is that input valid? Is the request authorized to begin with—and there have to be certain checks and balances to ensure that it is a valid request to begin with. This means there have to be certain checks and balances to ensure that a valid request is coming in from the agencies.

Mr. BARNARD. For the record, I think it would be very helpful if you could explain to the subcommittee in more detail how the TFCS, utilizing the Fedwire or private wire transfer systems, could be used to electronically transfer Treasury funds offshore.

For example, are the TFCS operators currently allowed to make payments to accounts in tax havens or bank secrecy jurisdictions?

Mr. SIMONETTE. Mr. Chairman, we are not prepared at this time to provide information on that. We did not cover that aspect during our review. We would be pleased to obtain that information and provide it to the committee, and also perhaps Treasury could assist in explaining for the committee how that process works, or that part of the process.

[The information follows:]

Our understanding is that the FEDWIRE system is not directly linked to any banks outside the United States. If a person wants to transfer funds to an institution outside the U.S. using the FEDWIRE, then they must first identify a correspondent bank in the U.S. to transfer the funds out of the country. This is normally done using the Society for Worldwide Interbank Financial Telecommunications

(SWIFT) and/or the Clearinghouse for Interbank Payments System (CHIPS) systems. Since it depends on which bank the funds are to be transferred to, the number of transactions necessary to get money from the U.S. to an offshore bank may vary. For example, if the transfer is to be made to a U.S. bank that has an overseas branch, then probably only 2 transactions, assuming FEDWIRE was used, would be necessary—one on the FEDWIRE system to transfer the funds to the U.S. bank and then one to transfer it from the U.S. bank to its overseas branch. However, if the foreign bank does not have a U.S. correspondent or the U.S. correspondent is not used, then several transactions may be necessary.

Mr. BARNARD. On page 7 of the IG's testimony, reference is made to former Secretary Regan's Treasury Directory 81-80 requiring proper authentication of all EFT transactions to and from Treasury by June 1, 1988. Is the authentication system proposed by Secretary Regan as good as the electronic certification recommended by the GAO and the IG?

Mr. SIMONETTE. Mr. Chairman, we believe that the proposal made by Secretary Regan does not go quite far enough. What we envision is electronic certification that would apply to basically all payments, not just the electronic payments. Certainly fraudulent activities have taken place in the check environment and, again, the same question arises as to the authenticity of the payment request.

If I might, Chris Martin has worked closely with the Treasury working group that is studying electronic certification, and I'd like to ask him to further comment on that.

Mr. BARNARD. Mr. Martin, if you would, how about also—if you have it available—tell us something about what the cost of the authentication system is and whether or not it's presently on schedule.

Mr. MARTIN. We don't have any cost estimates at this time. Treasury is developing a pilot project to test electronic certification, and part of that study is to come up with cost estimates.

There has been one study, which we have not reviewed in detail, that does a conceptual framework and does provide some cost estimates, but we are not prepared at this time to address the adequacy of those estimates.

Our understanding of 81-80 is that it is currently being redrafted and issued into a Treasury order. It also only covers message authentication and not electronic certification. There can be two different mechanisms used for message authentication and electronic certification.

We do not think the Treasury directive goes far enough because it only covers electronic payments and does not cover paper documents. Thus, it depends on what you define as an electronic payment. For example, a tape is an electronic payment. Our concern is that all payments should be equally subject to the same scrutiny.

Mr. BARNARD. I think I've already asked you whether or not you have got any estimates of any of the losses, and I believe you said you didn't have at this particular time, do you?

Mr. SIMONETTE. That's correct, Mr. Chairman.

Mr. BARNARD. Mr. Simonette, how many officials are there throughout the Government who are authorized certifying officers for the purpose of making payments?

Mr. SIMONETTE. Our understanding is that there is in the neighborhood of 6,000 to 7,000 certifying officers operating in the Federal agencies.

Mr. BARNARD. In how many localities do these individuals work?

Mr. SIMONETTE. I don't know if we have that information available.

Mr. KRAWCHYK. Again, that's a nationwide type of operation, and I don't think we could address the number of localities.

Mr. BARNARD. Your audit work only involved Federal civilian agencies. Do the payment systems of the Department of Defense bear any resemblance to the Treasury systems, and are they similarly vulnerable?

Mr. SIMONETTE. Yes, Mr. Chairman, they do bear a resemblance. I might point out that the Defense Establishment does use the TFCS system for the payments that meet that criterion, and in that regard Defense agencies are essentially using the same procedures to process payments through TFCS, including using certified payment requests.

We have not specifically examined this aspect in the Defense agencies, but we believe that since this is a Government-wide problem, we feel that the vulnerabilities that would be there are comparable to civil agencies.

Mr. BARNARD. Have you communicated your study to the Department of Defense?

Mr. SIMONETTE. We have not to date done that. We do have work planned in the Department of Defense. We have continuing work, as a matter of fact, in their various payment systems. We have not specifically communicated this report to Defense, but we will be working toward that in the near future.

Mr. BARNARD. There's really no other agency that you could go to that would have established a system that you would think would be adequate at this time, since all of them are processed through the Treasury—right?

Mr. SIMONETTE. That's our understanding; yes, sir.

Mr. BARNARD. Do you have any questions?

Mr. FISHER. No, Mr. Chairman.

Mr. BARNARD. Thank you very much, Mr. Simonette and gentlemen. We appreciate very much the study that you've made as well as you being with us today.

Mr. SIMONETTE. Thank you, Mr. Chairman.

Mr. BARNARD. Our next witness this morning is Mr. Michael R. Hill, who is the acting inspector general of the Department of the Treasury.

Mr. Hill, welcome to the hearing this morning. Thank you very much for cooperating with us in this study and in the followup on this GAO report.

At this time, you might want to introduce your associates that you have with you this morning.

STATEMENT OF MICHAEL R. HILL, ACTING INSPECTOR GENERAL, DEPARTMENT OF THE TREASURY, ACCOMPANIED BY ROBERT P. CESCA, ASSISTANT INSPECTOR GENERAL FOR FISCAL SERVICES AND ADP, AND MAURICE S. MOODY, DIRECTOR OF AUDIT, FINANCIAL MANAGEMENT SERVICE

Mr. HILL. Thank you, sir.

Mr. Chairman, it is indeed a pleasure for me to appear before you today to discuss an issue that concerns all of us in the Department of the Treasury. But, before I begin, may I introduce the other gentlemen who are accompanying me. On my left is Mr. Robert P. Cesca, assistant inspector general for Fiscal Services and ADP, and to my right is Mr. Maurice S. Moody, Director of Audit for the Financial Management Service.

At this time, Mr. Chairman, I would like to briefly summarize, one, the results of audits and investigations concerning internal accounting and physical controls over the manual and computerized network that the Government uses to disburse approximately $1 trillion annually; two, the actions taken to correct identified weaknesses; and, three, the use of electronic message authentication techniques to further protect the Government's payment mechanisms.

My testimony will be necessarily general due to the highly sensitive nature of how the payment mechanisms operate. In this regard, Mr. Chairman, we ask that any specific questions you or members of the subcommittee would like to ask on how the payment mechanisms operate or the details of our audit and investigative findings be deferred to a closed session.

Mr. BARNARD. It will be done.

Mr. HILL. Thank you, sir.

The Department's Financial Management Service (FMS) is responsible for issuing over 730 million payments each year, of which approximately 500 million are by check and approximately 230 million are by electronic funds transfer to financial institutions. About 115 million payments amounting to $440 billion are made directly by other agencies. The FMS disbursement process is carried out by seven financial centers located throughout the United States. All of the centers issue checks directly to payees and provide computer-generated tapes to the financial industry's automated clearinghouse system for making recurring payments into recipients' checking or savings accounts at financial institutions.

In addition, three of the centers have the capability to telecommunicate payment data directly to the Federal Reserve's Fedwire transfer system. The latter process is called the Treasury Financial Communications System [TFCS]. FMS generates payments through TFCS by using paper listings from authorizing agencies to input data at the financial centers; and by telecommunications from other Federal agencies directly to the TFCS network at the centers; 26 Federal agencies have direct access to TFCS through computer terminals.

While the rest of my statement addresses payment mechanisms, the subcommittee should be made aware that data on Treasury's annual collections of about $900 billion are also obtained from fi-

nancial institutions on computer-generated tapes and through TFCS.

Although the financial centers have extensive physical security and internal accounting control systems, flaws have been identified and occasional frauds have been perpetrated by individuals who have forged signatures and altered listings. I would like to point out, Mr. Chairman, that none of the known crimes in which funds were fraudulently obtained from Treasury had been carried out through penetration or circumvention of the TFCS. The frauds that have been detected were primarily in the check payment system and were accomplished by forgery or alteration of listings at the certifying agency and, as in one instance, by Treasury employees.

Even the most secure system is only as good as the controls over data provided by the officials who authorize payments. For example, in a case currently under investigation by the U.S. Secret Service, an authorized official prepared a false listing that was approved for payment by the recognized certifying officer and submitted to FMS for payment. The document was processed and the payment was made routinely by one of FMS's financial centers because the documentation met all of the established criteria for authorizing FMS to make the payment.

In another instance, a group of four people, two of whom were Treasury employees, altered listings and forged signatures on authorizing documentation for issuance of two checks. The perpetrators were successful in defrauding the Government of more than $800,000. Treasury's check payment and reconciliation system detected this fraud and the ensuing investigation by the Secret Service resulted in arrests and convictions.

To help ensure the integrity of payment mechanisms, two carefully controlled tests of the Treasury check disbursement system were conducted by the Office of Inspector General with FMS assistance during 1981 and 1982. In the first test, 29 false listings were submitted in the name of four internal Treasury accounting stations to a financial center. The false listings authorized issuance of 37 checks totaling about $187,000. Nine of the listings were rejected, while the other 20 were processed and checks totaling $123,000 were printed. Afterward, three of the four accounting stations detected and reported the unauthorized payments.

Our second test, conducted under the auspices of the President's Council on Integrity and Efficiency, was coordinated with inspectors general at six Federal agencies and was carried out through three FMS financial centers. It showed that the authorizing agencies' reconciliation procedures did not routinely provide for timely detection of false listings that were returned to them as paid. Nonetheless, of 85 fictitious listings submitted to the agencies, 81 were eventually detected by them.

In the first test, fictitious payees were used with addresses provided by the Secret Service. On completion of the test the checks were obtained from the Secret Service and canceled. During the second test, checks were also printed by the financial centers but were not issued. With the cooperation of FMS disbursing personnel, the checks were secured at the centers until the test was terminated and the checks were then canceled.

50-122 O - 86 - 2

Our report on these tests recommended nine corrective actions to help protect the payment system from risks such as those revealed by the tests. So far, seven of the recommendations have been implemented and two are still open.

We recently completed audits of the Service's ADP security program and the physical and administrative controls over electronic operations at four financial centers. During these audits we found that some weaknesses existed in operations, documentation, and physical and administrative security. FMS agreed with our findings and is in the process of correcting the problems.

Also, as the subcommittee is aware, GAO has issued a restricted report on TFCS in which one of its concerns pertained to potential risks to the system because of a specific weakness observed in one center's internal controls. The weakness cited by GAO was immediately corrected by the center, but to ensure that no improprieties occurred, we are confirming with the agencies who processed payments during the period in question that all transactions have been reconciled and any differences have been fully resolved. To date, 67 percent of the agencies have responded and none of them has reported a discrepancy.

Based on these findings and our ongoing reviews of Treasury's payment mechanisms, we believe that the most vulnerable stage of the process at present is during the flow of data from the agencies to FMS's financial centers and from the financial centers to the financial community. Within the Federal Government, most of the payment information sent from agencies to Treasury is by paper listings and computer tapes. The actual payments are made by paper checks prepared at the financial centers and by electronic funds transfer—EFT—through automated clearinghouses and the Fedwire system. The EFT payments are accomplished in two ways: First, by providing the automated clearinghouses with computer tapes; and, second, by computer telecommunications to the Fedwire system.

In recognition of the inherent vulnerabilities of the EFT systems, former Secretary Regan issued Treasury Directive 81-80 on August 16, 1984, requiring that all EFT transactions to and from Treasury be properly authenticated. All Federal EFT systems are expected to comply with TD 81-80 by June 1, 1988. In addition, Federal systems designed after August 16, 1984, must be in compliance with the directive. TD 81-80 defines EFT transactions as the movement of value from one party to another by electronic means, thus encompassing both computer tapes and telecommunications.

Very briefly, message authentication techniques include check digits, parity checks, cash totals, and authentication codes. The use of authentication codes is probably the most reliable method for ensuring that nothing is added, deleted, or altered in the text of a message, and it is the method being pursued under TD 81-80. To fulfill Treasury's responsibilities under TD 81-80, an electronic funds transfer certification task force was appointed to act as a forum for developing certification criteria and evaluating authentication devices and techniques.

I understand that Commissioner Douglas will be testifying on the task force's progress, so with your permission I would like to avoid preempting his statement by simply mentioning that our office is

represented on the task force and has been involved in this initiative since its inception.

One point I want to make is that while message authentication will help protect computer-generated data, it does not resolve the problems inherent with paper listings. But, if properly implemented, message authentication can provide positive identification of the sender. Therefore, Treasury's task force is working closely with GAO and the Federal agencies that generate payment data to develop requirements for using authentication as an electronic signature certification to replace the handwritten signature now used on paper documents. This will eliminate the need for manually prepared documents and enable agencies to eventually transmit all payment data electronically.

In our opinion, authentication technology and its use as an electronic signature certification offers much promise for improving security in the payment process. However, we must not allow ourselves to be lulled into a false sense of security because electronic payment systems are subject to many of the risks associated with manual payment systems. In fact, the greatest potential risk of loss will be presented by employees of the organizations using the electronic systems. Accordingly, each user organization must address security issues relating to the integrity of employees who participate anywhere in the cycle of generating, receiving, verifying, or approving data for payment systems.

This concludes my prepared statement Mr. Chairman.

Mr. BARNARD. Thank you, sir.

Mr. Hill, you indicate that your office made two tests, and while the numbers don't seem to be all that extensive from the standpoint of failures, on the other hand, the vulnerabilities could be tremendous. How do you evaluate the tests that you made? Do you feel they were adequate?

Mr. HILL. I think the tests were adequate; yes, sir. I think we identified what objectives we planned to fulfill in those audits, and I believe that we accomplished those objectives; yes, sir.

Mr. BARNARD. Mr. Hill, in your testimony you gave us some examples of actual thefts against the Treasury system. For instance, you described two fraudulent checks being issued for more than $800,000. You also described two audit tests conducted by your office in 1981 and 1982 where many checks were issued based on false payment lists.

In the $800,000 theft, how long was it before the thefts were detected, and how were they detected?

Mr. HILL. I respectfully request your permission to respond to that question for the record at a future date.

Mr. BARNARD. All right.

[The information follows:]

The $800,000 was fraudulently obtained through two crimes that were carried out by the same individuals during the period October through December 1983. One of the fraudulently issued checks was identified by the Treasury Check Payment and Reconciliation System within 2 months after it was issued. This was referred to the Secret Service and the resulting investigation eventually led to discovery of the other fraudulently issued check.

Mr. BARNARD. Mr. Hill, on page 3 of your testimony, you state that none of the known crimes in which funds were fraudulently

obtained from Treasury have been carried out through penetration or circumvention of the TFCS, that the thefts detected were primarily in the check payment system. Given what you know about how the check payment frauds were committed, is there any reason to believe that they couldn't have been committed just as easily against TFCS?

In other words, can't the TFCS currently be broken into in the same way that the check payment system has already been broken into?

Mr. MOODY. If I may, Mr. Chairman.

Mr. BARNARD. Mr. Moody.

Mr. MOODY. Typically, a TFCS transaction is also generated by a paper listing, which is processed and signed just as one would be for a paper check. In that regard, one can submit false documentation into the TFCS input process and have a payment generated. That's correct.

In reference to the penetration or circumvention of TFCS, we have no known cases of someone from a remote location gaining access to the secure system or penetrating the telecommunications network during transmission.

Mr. BARNARD. Would you say that, given the vulnerabilities in the present payment system, it seems that a great deal is riding on the speed and adequacy by which authorizations for payments are reconciled with the payments themselves?

Mr. MOODY. I would say yes.

Mr. BARNARD. How much faith do you have in the speed and adequacy of the reconciliation process?

Mr. HILL. I think we'd prefer to respond for the record on these questions, if we could, Mr. Chairman.

Mr. BARNARD. All right.

[The information follows:]

It is difficult for us to draw a conclusion about the speed and accuracy of the reconciliation processes currently performed by the other agencies. To render an opinion, we would need the benefit of audit findings from the respective Inspectors General or internal audit staffs concerning the effectiveness of corrective actions taken for the problems cited in our report on the Government-wide review of check disbursement systems.

In that report, we cited several problems involving the speed and accuracy of the agencies' reconciliation processes, and we recommended a number of changes in the policies and procedures manual that Treasury provides to other Federal agencies. The Department implemented our recommendations by providing the necessary emphasis and guidance to the other agencies concerning reconciliation of "paid" listings sent to them from the financial centers.

Although a Government-wide follow-up study has not been performed we have received input that some of the agencies are reviewing the adequacy of their current reconciliation processes in connection with our request for verification of TFCS payments.

Mr. BARNARD. Let me ask you this question, Mr. Hill. Of the nine recommendations resulting from your two audit tests in 1981 and 1982, two are still open. Could you explain what these are and why they haven't been implemented?

Mr. HILL. Yes, sir; I will let Mr. Moody handle that question.

Mr. MOODY. The first recommendation referred to a listing which is used for processing the payment. Our proposal was that these listings be prenumbered and that controls be maintained over the

numbered listings. These documents have been printed and are available, but have not been given to the agencies for use.

The second recommendation was that FMS perform edits of these listings when the financial centers receive them to detect breaks in the numbering sequence and to ensure that the number of the current payment authorization begins where the last one left off. So implementation of the second recommendation is dependent on implementation of the first recommendation.

My general understanding—I'm sure Commissioner Douglas can speak more specifically about this—is that the intent now within FMS is to begin using the new documents on approximately June 1, 1986, with the edit tests likely to begin in October 1986.

Mr. BARNARD. Mr. Hill, the subcommittee in its oversight of the IRS has conducted a number of hearings into the subject of tax evasion through the use of offshore tax havens and bank secrecy jurisdictions like the Netherlands Antilles, the Bahamas, and Panama. Once U.S. source income is sent to these type nations, the money is gone and the ability to determine who owns it is practically nonexistent.

Can you explain to the subcommittee in more detail how the TFCS, utilizing the Fedwire or private wire transfer systems could be used to electronically transfer Treasury funds offshore?

Mr. HILL. Again, I would prefer to respond to that for the record, sir.

Mr. BARNARD. OK. Well, we'll try again.

[The information follows:]

The TFCS does not transfer payment data to foreign countries. However, after a TFCS deposit is made domestically, the recipient of Federal funds could instruct the financial institution to transfer monies from his or her personal account to an account in another country using a private wire transfer system.

Mr. BARNARD. Mr. Hill, what was the extent of FMS's efforts to verify the signatures of the payment listings on the first audit tests you mention on page 5 of your testimony?

Mr. HILL. I'll let Mr. Moody handle that question, sir.

Mr. MOODY. The processing clerks were not aware of the tests so the extent of verification was not changed from the normal routine within the respective financial centers. We have observed the process during several audits.

What is required of the employees at a center is that a verification be made of each signature on a document against a sample of the certifying officer's signature that they have on file. In several cases, because of the high volume of transactions, we observed that the clerks were not exercising this requirement 100 percent, and therefore would only confirm a sample of the signatures within a pile of vouchers. Overall, we observed that signature verification was being performed; however, we felt it could be much better.

Another problem cited in the report, for which we recommended corrective action that was taken by FMS, related to the recency and the authenticity of the financial centers signature files—when I say authenticity, I am referring to an official form from a Government agency that designates the certifying officer and contains a sample of his or her signature.

Mr. BARNARD. How many of those signatures are on file?

Mr. MOODY. There is a signature on file for every certifying officer; approximately 7,000.

Mr. BARNARD. 7,000.

Mr. MOODY. Among the seven financial centers, yes.

Mr. BARNARD. Mr. Hill, your testimony refers to 26 agencies that have direct access to TFCS through computer terminals. How is this access controlled and authenticated?

Mr. HILL. Mr. Moody will respond, sir.

Mr. MOODY. The TFCS operations in the three financial centers are in physically secured areas that can only be entered by using cypher locks or card access equipment. The supervisors are located in or near the TFCS operations rooms during processing and the rooms also have adequate visual observations through glass windows so that other individuals in the center can see who is in the TFCS room. The TFCS computer is housed in a controlled vault in Washington, DC, so no one can enter unless he or she is authorized to assess the computer hardware. The operations within the centers are separated so that clerks perform different functions. The system of internal controls is to prevent one person from doing another's function.

The example GAO referred to in one center resulted from a temporary breakdown of internal controls, but we are confirming the transactions and, to date, we have reasonably good evidence that no improprieties occurred in the payment process at that time.

Mr. BARNARD. Let me refer back to this other question that I asked you about authentication. Aren't there some technological improvements today that would make it easier to authenticate the authorizations other than just visual signature comparison?

Mr. MOODY. Yes; there is a process under authentication techniques that is called a message authentication code, where a so-called black box is used—it can be a hand-held unit or an add-on to a computer system—that would take certain data fields from the original document and develop, through the use of an algorithm, a unique code that can then be placed on the document or computer tape or in the telecommunications signal. The receiver then has a key to determine that the code has not been changed.

In other words, when it's read out at the other end, a similar device is used to read the data and independently compute a code which should be identical to the code put on the communication by the sender. If the code has been changed, that means someone has tampered with the information.

Mr. BARNARD. But that is done strictly with a code—right?

Mr. MOODY. Yes, sir; the assignment of a code.

Mr. BARNARD. All right. What about actually reading a signature? Aren't there some computers which can read signatures?

Mr. MOODY. There is technology available to read the handwritten signature through optics; yes, sir. To my knowledge, it's very expensive, and it is not 100-percent reliable, but neither is the present visual inspection, as you are well aware.

Mr. BARNARD. All right. One further question.

Mr. Hill, the GAO just testified that former Secretary Regan's authentication program is not absolutely satisfactory. Do you agree?

Mr. HILL. I would prefer to respond for the record, sir.

[The information follows:]

GAO's concern, as I understand it, is that TD 81-80 does not specifically address electronic signature certification. However, I believe the criticism of Treasury's initiative may be premature because, as I mentioned in my prepared statement, the Department's Electronic Transfer Certification Task Force is working closely with GAO and the Federal agencies that generate payment data to develop requirements for using authentication as an electronic signature certification.

Mr. BARNARD. The information that you used to conduct your tests—were you specially privy to that information, or is that something anyone could have access to?

Mr. HILL. I'm not sure what information you are——

Mr. BARNARD. In other words, you conducted several tests. Did you use public information, or was that special information?

Mr. HILL. Most of it was public information, sir.

Mr. BARNARD. Thank you very much, gentlemen. We appreciate very much your being here today and offering this testimony. If you would remain after the next witness, we will probably go into executive session for some further questions.

Mr. HILL. Thank you, sir.

Mr. BARNARD. Our next witness this morning is Mr. William E. Douglas, Commissioner of the Financial Management Service, Department of the Treasury.

Mr. Douglas, I'm glad to say that you're not the Acting Commissioner, that you are the Commissioner. From time to time we've had a lot of acting come before our committee. So I'm glad that you're in place and functioning.

Mr. DOUGLAS. Thank you, sir.

Mr. BARNARD. Mr. Douglas, I see you have with you this morning Mr. Page, and I would appreciate if you would introduce him as you offer your testimony.

STATEMENT OF WILLIAM E. DOUGLAS, COMMISSIONER, FINANCIAL MANAGEMENT SERVICE, DEPARTMENT OF THE TREASURY, ACCOMPANIED BY MARCUS PAGE, DEPUTY COMMISSIONER

Mr. DOUGLAS. Thank you, Mr. Chairman.

On my left is Marcus Page, who is the Deputy Commissioner of the Financial Management Service.

Mr. BARNARD. Mr. Page, we welcome you this morning.

Mr. PAGE. Thank you, Mr. Chairman.

Mr. DOUGLAS. Mr. Chairman and members of the subcommittee, I welcome this opportunity to respond to the subcommittee's concern about the Treasury Financial Communications System and the recommendations for electronic certification.

The Treasury Financial Communications System [TFCS] is the U.S. Treasury Department's electronic funds transfer link between Federal agencies and the Federal Reserve bank communications system known as Fedwire. TFCS is used for large, nonrecurring payments. In addition, deposit information for large deposits electronically transferred to Treasury's account with the Federal Reserve banks is made available to agencies through TFCS. It is not used, however, for recurring payments such as Social Security benefits, veterans' benefits, and the like.

It is very important the following facts be emphasized:

First, the TFCS control center is housed in the Treasury Annex vault, a highly secured facility containing a sophisticated set of fire, security, and protective systems. Access is very restricted, and the site offers a high degree of functionality and protection.

There is no evidence that security for the Treasury Financial Communications System has ever been breached during its 10 years of operation.

Third, there is no evidence that anyone has improperly used the system to divert or steal any money from the Government, not $1.

Fourth, the GAO audit report, issued in September 1985, found no losses resulting from security breakdowns but made 14 recommendations for improvement in systems operations.

We agreed with all but two recommendations, have completed nine, and the remaining three, which are mostly additional system edits, are in progress.

Treasury's first formal look at electronic certification came as part of the payments mechanism study which the Financial Management Service conducted in 1982 and 1983. The report recommended that FMS begin to look at electronic certification as a part of its overall electronic funds transfer system.

In August 1984, the Treasury Department issued a directive requiring all Federal funds transfers to be protected by message authentication under ANSI Standard X9.9 by 1988. We then established an EFT task force with representatives from Treasury, GAO, and the National Bureau of Standards to determine criteria for approving vendor hardware systems for electronic certification and message authentication. A detailed outline of this initiative is submitted for the record.

[Attachment 1 follows:]

Attachment 1

HISTORICAL BACKGROUND
ELECTRONIC CERTIFICATION
FINANCIAL MANAGEMENT SERVICE

Treasury's first formal look at electronic certification came as part of a Payments Mechanisms Study that began in 1982 and concluded with the a final report in June 1983. This study, carried out by Deloitte, Haskins, and Sells, looked at Treasury's overall payments systems, examined similar and alternative systems used in the private sector, and produced a series of recommendations that were made part of Treasury's strategic planning for improving its payments systems. The report recommended that Treasury begin to look at electronic certification as a part of overall electronic funds transfer.

Treasury began its systems development life cycle approach with a contract award in November 1983 to American Management Systems to develop a requirements analysis for an integrated payment system that would include electronic certification and message authentication for Federal payments. In February 1984, Treasury met with GAO staff to begin discussions regarding electronic certification, its legality, its impact on certifying and disbursing officer liabilities, and the method that would produce the highest level of security for the dollar invested. In September 1984, the GAO General Counsel issued a legal opinion clearing the way for development of an electronic certification system. Treasury proceeded with award of contracts to Orkand Corporation to develop a design for an integrated payments system, including telecommunications of payment data, electronic certification, and message authentication. Orkand completed the design for the integrated payment system in June 1985. The recommendations included a proposed electronic certification pilot between FMS' Birmingham Regional Financial Center and the Department of Agriculture's National Financial Center in New Orleans. The pilot would require a 4300 type computer and $600,000. This proposal was beyond FMS resources.

Paralleling the contractor efforts, the Treasury Department issued in August of 1984 a directive titled, Electronic Funds and Securities Transfer Policy-Message Authentication. This directive requires all Federal funds transfers to be protected by message authentication under ANSI Standard X9.9 by 1988. Shortly after issue of the Treasury directive, an EFT Task Force was established with representatives from Treasury, GAO, and NBS to establish criteria for approving vendor hardware systems for electronic certification and message authentication.

A contractor is currently developing a proposal for an electronic certification pilot between two accounting offices in Washington and the Washington Financial Center. Vendor payment records will be transmitted under message authentication with an electronic certification. The two-stage pilot could begin this fall if funding is available.

After the pilot, full implementation will depend on the development of a telecommunications network between 6,000 certifying officers at 900 locations nationwide and Treasury's seven Regional Financial Centers. In addition, we must replace our 1960's and 1970's style computers with systems incorporating current technologies. We believe full implementation could occur within two years of network availability.

Mr. DOUGLAS. The status of Treasury's electronic certification process as of today is as follows:

The EFT task force has completed criteria for electronic certification and message authentication. Certifying devices should be available in the May-June 1986 timeframe.

A contractor is currently developing a proposal for an electronic certification pilot between two accounting offices in Washington and the Washington financial center. Vendor payment records will be transmitted under message authentication with electronic certification. The two-stage pilot could begin this fall if funding is available.

After the pilot, full implementation will depend on the development of a telecommunications network between 6,000 certifying officers at 900 locations nationwide and Treasury's 7 regional financial centers. In addition, we must replace our 1960's and 1970's style computers with systems incorporating current technologies. We believe full implementation could occur within 2 years of network availability. A breakdown of estimated costs is submitted for the record.

[Attachment 2 follows:]

Attachment 2

ELECTRONIC CERTIFICATION
ESTIMATED IMPLEMENTATION COSTS

Based on contractor projected costs, implementation will cost about $31 million. Breakdown of costs is as follows:

- Computer equipment to support a major telecommunications system, electronic certification, message authentication, key management, and integrated payment systems -- $20 million *
- Integrated Payments System Software -- $ 3 million
- Telecommunications cost annually -- $ 4 - 5 million
- Smart card readers, smart cards, and system software (900 locations) -- $ .6 million
- Message authentication devices and software (900 locations) -- $ 2.5 million
- Treasury Security and Operating Personnel cost -- $ .5 million

This does not include agency personnel at the 900 agency locations.

* Approximately $17 million of this amount will be needed by FY '88 in order to replace 1960's and 1970's computers in the Financial Centers.

Mr. DOUGLAS. I would like to conclude my statement by reemphasizing three points.

First, Treasury has had no security-related losses in TFCS. Although a few cases of abuse have been documented in the check issue system, considering that FMS issues some 500 million checks each year, the record has been exceptional.

Second, although no losses have been experienced in TFCS, we agree with the General Accounting Office that the growth of EFT brings with it the possibility of large dollar losses. We also agree that signature verification is obsolete in terms of both security and operational considerations.

Third, the investment to provide the needed computer support system as well as electronic certification integrated with message authentication in an overall electronic funds transfer system is substantial, but we believe that the investment is necessary.

We appreciate the interest of the subcommittee in improving the security of the Government's payment systems, and we welcome your support in moving toward that objective.

Mr. BARNARD. Thank you, Mr. Douglas.

Mr. Douglas, your prepared statement acknowledges that electronic funds transfer brings with it the possibility for large value losses, but it paints a rather positive picture of the TFCS. Very frankly, this picture is at odds not only with the GAO and IG testimony but with a quality assurance letter that you wrote back on October 31, 1985, to Treasury Secretary Baker. Are you familiar with that letter?

Mr. DOUGLAS. Yes, sir, I am.

Mr. BARNARD. I won't quote from it then.

Well, would you please respond to your own expressions of concern in your October 31 letter?

Mr. DOUGLAS. Yes, sir, Mr. Chairman. I do not believe that we really have a different view from the GAO or the IG since both of those organizations have done extensive reviews and both of them, I think, have stated that they know of no losses through TFCS, and indeed the controls features—and we have full levels of controls in that system—would reveal any such losses had they occurred.

My reservations about a full assurance to the Secretary involved not just TFCS nor indeed not just the payment systems, but it involved extensive reviews of all of our internal controls and all of our vulnerabilities through the Financial Management Service, and we looked at literally thousands of points that could potentially have been weaknesses. Because I had some concerns about those, and I do have some concerns about TFCS, I believe the security can be enhanced, and I am very supportive of the argument that is made by GAO that electronic certification is a better way to prevent unauthorized or fraudulent payments. In fact, we began the exploration of that technology several years before the GAO's review.

Mr. BARNARD. Mr. Douglas, in your quality assurance letter you voiced some concern about the sufficiency of budget resources. Can you comment this morning on whether or not you have enough funds to do all of the essential things that need to be done to improve security in the payment system?

Mr. DOUGLAS. Mr. Chairman, as you know, not only this year but in prior years the budget picture has not been a bright one. Receiving the funds necessary to do the job as well as we would like to do it is a very difficult process. I would say that we have some needs. I think in my letter to the Secretary I pointed out that our Quality Assurance Division, for example, was still not staffed sufficiently. We have system changes that we need to make, and they require resources.

Could I use some more resources to heighten the security levels? Yes, sir, I could.

Mr. BARNARD. Mr. Douglas, can you elaborate a little bit further at this time on any proposals that you are making to overcome TFCS' vulnerability to forged signatures and altered lists?

Mr. DOUGLAS. A major concern there, Mr. Chairman, is the security, the controls, not in our own operation in TFCS but on the transmission of certifying information to us from the agencies. We agree with GAO, we agree with the IG, that if we could combine electronic certification technology with message authentication we would significantly increase the security of payment messages coming in, and that would be true of checks as well.

Mr. BARNARD. Have you found a system that would accommodate that?

Mr. DOUGLAS. We are working on such a system. I mentioned in my remarks that we believe devices will be available to us probably early this summer, and we would be prepared to do a test, or a pilot test, some time this fall if we had the funding.

Mr. BARNARD. Again I want to ask you, are you concerned about the funding for this particular——

Mr. DOUGLAS. Yes, sir.

This technology is not inexpensive, but, as you pointed out in your remarks, we're talking about hundreds of billions of dollars.

Mr. BARNARD. It wouldn't take too many losses, though, to more than pay for the system.

Mr. DOUGLAS. That's right, sir.

Mr. BARNARD. I've asked a similar question of other panelists this morning, Mr. Douglas, but this subcommittee has conducted a number of hearings into the subject of tax evasion through the use of offshore tax havens and bank secrecy jurisdictions. As we have indicated, once the U.S. source income is sent to these type nations, the money is gone and the ability to determine who owns it is practically nonexistent.

Can you explain to the subcommittee in more detail how the TFCS, utilizing the Fedwire, private wire, transfer system, could be used to electronically transfer Treasury funds offshore, or would you rather wait and do that?

Mr. DOUGLAS. My answer, sir, is that TFCS connects to the Federal Reserve's Fedwire system, and our funds transfers, which are encrypted, on encrypted lines, go either to the New York Fed or to the Richmond Fed.

The Federal Reserve System, their EFT system, does not operate overseas. There is an overseas EFT system—it's called SWIFT—which is operated by some European and American banks, but the Fed system does not connect to that, so that it would not be possi-

ble to make a transfer into a foreign account directly through TFCS.

Mr. BARNARD. That's the point we're trying to pursue, that these payments could eventually get to an offshore——

Mr. DOUGLAS. Through a series of transactions, it is possible.

Mr. BARNARD. The staff director said, as a matter of time, it would take very, very little time to do that—I mean, practically instantaneously in today's technology.

Mr. DOUGLAS. It would take several transactions though. It would have to come out of the Fed system into another account and then be moved through another system. There is no direct means of transferring through EFT to a foreign bank, through the Fed system.

Mr. BARNARD. How much time would that take?

Mr. DOUGLAS. I have no idea. It would depend on the arrangements that were made into an account and then through another system. It would be speculation.

Mr. BARNARD. I have no further questions at this time, Mr. Douglas. Just one second though.

Mr. Douglas, we would assume that your security reviews are ongoing. What is the number of vulnerability assessment audit reviews that you have made in the past year?

Mr. DOUGLAS. This past year, 1985, Mr. Chairman, we made well over 100 reviews, vulnerability assessments, in attempts to see any points throughout our systems that might have some weakness.

Mr. BARNARD. The other question is, do you have any funds in the fiscal year 1987 budget to complete the installation nationwide of your electronic certification network?

Mr. DOUGLAS. No, sir, we do not. I mentioned earlier that such a system would require a substantial investment. A major portion of that, however, would be needed by us, because the computer systems that we have in our financial centers date back to the 1960's and 1970's, and we would have to have modern technology in order to support an electronic certification or message authentication technology. In addition, we would have to set up a network to be able to do that, and we have no funds to do either one of those things or to replace those computers in the fiscal year 1987 budget.

Mr. BARNARD. The Orkand study that you commissioned indicates that you still haven't fully installed new computers you purchased in 1984. Apparently these will have to be replaced again for electronic certification.

Mr. DOUGLAS. That's not quite correct, sir. We do use—they happen to be Honeywell 6680 computers, which we got as a stopgap, sort of a bridge, in the first part of the 1980's, and they are in use, and in fact the new paper checks that we are using that are going out to Social Security recipients, tax refund recipients, now, are produced through the Honeywell system.

Mr. BARNARD. So, in other words, the equipment purchased in 1984 is being used?

Mr. DOUGLAS. Yes, sir, it is being used, but it is 1970's technology. It was a bridge.

Mr. BARNARD. 1970?

Mr. DOUGLAS. It's 1970's—it's probably 1975–1976 level.

Mr. BARNARD. You are going to have to replace that eventually.

Mr. DOUGLAS. Yes, sir. We did that because the other computers we had were at least 10 to 15 years, even older than that, and it was to get us over the hump until we could come in with a complete replacement system.

Mr. BARNARD. Can you give us your best estimate of when the certification system could be in place or will be in place?

Mr. DOUGLAS. As a pilot test or full-scale?

Mr. BARNARD. Full-scale.

Mr. DOUGLAS. Assuming that we were able to get the computer system and the telecommunications network to support that technology by, say, 1988, it would probably be 1 or 2 years after that.

Mr. BARNARD. Our staff director is exasperated because it's not being done tomorrow. I voted for Gramm-Rudman though.

Mr. DOUGLAS. I haven't looked at your staff director's wallet, but if he has a lot of money, he could certainly help us out.

Mr. BARNARD. He has. He says he can get the money through your system.

Mr. DOUGLAS. Well, no one else has been successful; so we wish him well.

Mr. BARNARD. I don't think he'll be doing that, frankly.

All right, sir. With that, Mr. Douglas, why don't you remain; Mr. Page is welcome to remain, too; and then we'll have Mr. Simonette and Mr. Hill to join you at the table.

With that, without objection, we will then go into executive session, and I will respectfully request that anybody not a part of these hearings will kindly adjourn.

[Whereupon, at 11:10 a.m., the subcommittee adjourned and proceeded to go into executive session.]

APPENDIXES

APPENDIX 1.—RESPONSES BY JOHN F. SIMONETTE, ASSOCIATE DIRECTOR, ACCOUNTING AND FINANCIAL MANAGEMENT DIVISION, GENERAL ACCOUNTING OFFICE, TO ADDITIONAL QUESTIONS SUBMITTED BY THE SUBCOMMITTEE

QUESTIONS RELATING TO TFCS

Question

The instances of fraudulent payments discussed in GAO's testimony involved Treasury checks. Do you believe that this type of fraud could have occurred with the Treasury Financial Communications System (TFCS)?

Response

The determination of whether a payment request should be processed is the same for all payment methods. Therefore, if a fradulent request is processed for checks, it is logical to assume, had TFCS been specified, that it could have been processed by TFCS.

Question

What controls should Treasury have to provide reasonable assurance that payment requests submitted to Treasury are authentic?

Response

It is the responsibility of Treasury to establish the disbursing rules and for the agencies to properly implement them. Because Treasury has the responsibility for issuing payments on behalf of many agencies, we believe it also has the responsibility to establish an appropriate level of control over how those payments are executed. For example, in

our report, we noted that TFCS did not have a duplicate payment edit and that one should be provided which would assist in detecting duplicate payments. Treasury initially stated that this was an agency responsibility but later determined that a duplicate payment edit should be included. We agree that agencies should have effective systems to prevent duplicate payments, however, Treasury should also have controls to reduce the number and amount of such payments. Although it may not be feasible for Treasury to audit the agencies' controls, it would be desirable for Treasury to obtain some type of assurances from the agencies that the prescribed controls are being followed. Under the Federal Managers' Financial Integrity Act, agency heads are already required to report annually on the adequacy of their controls. Treasury and OMB could work together to provide guidance to the agencies to ensure that disbursement controls and the related reconciliations are included in those evaluations. Treasury could also work with the agencies' Inspector General to encourage periodic audits of those operations.

Question

In the GAO report that was discussed in the testimony, several control weaknesses were identified which had not caused any actual losses but were still considered significant by GAO. Can you provide additional information on why these areas are important?

Response

Yes, effective internal control systems are designed to minimize the risk that losses will occur. When we review internal control systems, we evaluate the risks associated with each weakness identified. Therefore, actual losses do not have to occur in order to justify improving an agency's controls. A recent Department of Justice report on EFT fraud in the commercial sector highlighted several of the areas we found in our review. Examples of significant items include:

--Duplicate payment messages lead to 55 percent of fraudulent losses. Duplicate payment messages also accounted for 24 percent of the errors which did not result in a loss.

--The respondents to the Justice survey also cited that misuse of passwords contributes to 30 percent of the current cases of fraud and loss and it is expected to grow to 39 percent within five years.

--The respondents also stated that internal and external collusion were expected to increase significantly within the next five years.

One of the report's conclusions was that inadvertent errors, such as "typos" or misplaced digits, may result in a major loss if recipients of the erroneously credited payments abscond with the funds, claim legitimate receipt, or otherwise spend the windfall in alleged ignorance of the fund source. Recovery of such losses may be legally complex and costly.

Although our review of TFCS did not identify any similar cases which resulted in a loss, we pointed out a similar weaknesses and Treasury agreed to take actions to correct the problem.

Question

The report referred to above did not recommend that Treasury implement electronic certification. What was the reasoning behind this omission?

Response

We began to consider this as a feasible alternative as neared the end of our study. At that time, sufficient information on what would be needed to implement an effective electronic certification system was not available. Therefore, we chose to support the concept and Treasury's efforts toward this goal. We consider electronic certification and message authentication to be an important area and will continue to monitor Treasury's efforts.

Question

Exactly what elements should be in an electronic certification system installed at Treasury? Which of these elements are being considered by Treasury and which are not?

Response

That is a very difficult question to answer because the technology to implement a workable system is new and has

not been completely evaluated. Furthermore, we do not yet know how Treasury plans to implement its system. At this time we believe that an electronic certification and message authentication system should be integrated with the overall disbursement system and include such items as the following:

--A means to ensure that someone other than the certifying officer prepares manual payment requests.

--The ability to telecommunicate payment information with a high degree of assurance that it has not been tampered with either by agency personnel, outsiders, or Treasury officials.

--Adequate physical controls over payment documents and equipment as well as an evaluation of the personnel operating the system.

--A methodology that would relate risks to the type of equipment required and procedures implemented. For example, agencies which disburse large dollars should have a more effective system than smaller agencies which have smaller payments. In other words, the level of control exercised should be related to the amounts at risk.

--A method to identify which individuals authorized and certified individual payment.

--A mechanism that would ensure that no individual would know the key used for authenticating or certifying payments. Basically, only Treasury's computer and the

device used for authenticating or certifying the payment should have this information.

We recognize that these are broad areas and that many different controls will be needed to satisfy them. We also realize that several different system concepts may meet the above requirements.

We would also like to point out that Treasury has requested us to assist in the development of this system by commenting on their plans. We look forward to providing our views on their system as it is developed.

Question

How can a fraud be committed once electronic certification and message authentication have been implemented?

Response

If properly implemented, electronic certification and message authentication has the potential to provide improved controls over payment requests but it is not the total solution to preventing or reducing improper payments. For example, if an improper payment is not detected by the agency and is erroneously certified, the method of certification is irrelevant. Therefore, the agencies and Treasury will still need adequate internal controls to ensure that the payments that are being authenticated and certified are proper.

Question

In one of the fraud cases GAO discussed which resulted in a loss of $ 856,000, it was stated that electronic certification would have made the fraud more difficult. Please explain this statement in more detail.

Response

Since Treasury has not yet determined how electronic certification is going to be implemented, it is difficult to evaluate how effective it would be against a specific case. However, we assume that such a system will include the total number of payments being certified. Because the individual in the case you mentioned supposedly added the fraudulent payment to a request that was already certified, the discrepancy would have been discovered by Treasury when it began processing the request and compared the total number of payments certified to those on the voucher.

APPENDIX 2.—RESPONSES BY MICHAEL R. HILL, ACTING INSPECTOR GENERAL, DEPARTMENT OF THE TREASURY, TO ADDITIONAL QUESTIONS SUBMITTED BY THE SUBCOMMITTEE

OFFICE OF INSPECTOR GENERAL
DEPARTMENT OF THE TREASURY
RESPONSES TO QUESTIONS FROM THE
CHAIRMAN, SUBCOMMITTEE ON COMMERCE,
CONSUMER, AND MONETARY AFFAIRS
HOUSE COMMITTEE ON GOVERNMENT OPERATIONS

Question 1.

Your testimony provided some examples of actual thefts against the Treasury disbursement systems. For instance, on page four you describe two fraudulent checks being issued for more than $800,000. You also describe two audit tests conducted by your office in 1981 and 1982 where numerous checks were issued based on false payment lists.

a. In the $800,000 theft how long was it before the thefts were detected and how were they detected?

b. In the first of the two audit tests, how many checks were issued? What was the reason that nine of the listings were rejected? How many of the fraudulent checks were detected and what was the dollar amount?

How long did it take for each of these checks to be detected? How many checks for what dollar amount were undetected? Why were they undetected?

c. In the second of the two audit tests, what was the average number of days it took for the 81 listings to be detected? What was the range? How many checks for what dollar amount were on the listings that were eventually detected? How many checks for what dollar amount were on the four listings which were not detected?

Response:

The $800,000 was fraudulently obtained through two crimes that were carried out by the same individuals during the period October through December 1983. One of the fraudulently issued checks was identified by the Treasury Check Payment and Reconciliation System within two months after it was issued. This was referred to the Secret Service and the resulting investigation eventually led to discovery of the other fraudulently issued check.

In the first test 29 listings were prepared for the issuance of 37 checks and were submitted to a disbursing center during the period June 22 through July 17, 1981. Twenty of the listings were fully processed and 24 checks totalling $122,958.78 were issued.

The disbursing center's examiners detected deficiencies or flaws in only 9 of the 29 listings. Three listings were rejected by the disbursing center because of missing schedule and/or agency station numbers. One listing was rejected because the amount for an individual payee had been altered, but the total amount due all payees had not been changed. Five listings were rejected because of deficiencies in the certifying officers' signatures. In one, the signature of a former certifying officer had been used, and in another the certifying officer did not exist. A third was unsigned. Only two listings were rejected because of imperfections in the signature. In one, the signature evidenced a double impression, and in the other the middle initial was missing.

All of the 20 listings that were paid contained traced or otherwise falsified signatures. In addition, two of these listings contained obvious alterations in the payee amounts; two contained payments which had been added without altering the listing total; and three others contained names of former certifying officers. These listings were paid because of inadequate review procedures at the Center.

The second phase of the disbursing center test indicated serious weaknesses in accounting station procedures to detect checks issued as a result of fraudulent listings. One of the four accounting stations never detected the fictitious listing or the fact that nine unauthorized checks for $57,452.78 had been issued against its appropriations. The station had not compared the "paid" and "pending" copies of the listings. The three other stations detected the fictitious listings for 15 checks totalling $65,506, but it took an average of 7 days (6 days median) from the printing of the checks for them to do so, with delays ranging from 5 to 17 days.

In the second audit test, 85 false listings requesting issuance of 162 checks totalling $1,097,870.65 were processed and stamped "paid" by three disbursing centers. The listings were then sent to six agencies using the normal delivery methods for each agency. Five of the agencies detected 81 of the false listings sent to them on which 155 checks for $1,072,755.15 were shown as issued. However, the accounting stations took an average of 20 days (7 days median) from the printing of the checks to detection, with delays ranging from 3 to 51 days.

The sixth agency did not detect four listings showing that seven checks for $25,115.50 had been issued. The accounting station attributed its failure to identify the false listings to a recent reorganization within its region.

Question 2.

Your testimony states that no known funds have been fraudulently obtained through penetration or circumvention of the Treasury Financial Communication System (TFCS). The subcommittee has been informed by the Secret Service, however, that they are currently investigating a case where fraudulently prepared requests were signed by the appropriate certifying officer and payments were effected on TFCS. This apparently is the same case you alluded to on page four of your statement. Could you comment on this apparent contradiction?

Response:

The reference to TFCS was made in the context of an authorized or unauthorized person obtaining direct access to the TFCS terminals, computer hardware or telecommunications system to perpetrate a fraud. As was stated in the hearings, most of the known frauds occurred through falsification of input documents that were processed through the disbursing system undetected.

The case being investigated by the Secret Service involves a fraud where an authorized official prepared a request for a TFCS payment to a corporate account that he opened in a financial institution. The request was prepared on the required documents with proper identification codes or symbols and was processed through the review system of the authorizing agency undetected. The request was then signed by the agency's recognized certifying officer. Because the request complied with all of the criteria used during review at FMS, the TFCS payment was made.

Question 3.

On page six of your statement, you note that GAO has issued a restricted report on TFCS pointing out specific weaknesses at one disbursing center. You also stated that, to ensure that no improprieties had occurred, you are confirming with the agencies who processed payments during the period in question that all transactions have been reconciled and any differences have been fully resolved.

a. The subcommittee has been informed that the Financial Management Service received a draft of the GAO report in June of 1985. We also have learned that the confirmation effort did not begin until January of 1986. Could you explain the delay?

b. Do you think the passage of time from when payments were issued to the time of confirmation in any way diminished the reliability of the results you are receiving since some agencies may not even have the records on hand to do a proper verification?

c. Do you think the agencies are making a legitimate attempt to verify the payments, especially in view of the agencies' reconciliation problems you mentioned on page five of your statement?

Response:

GAO's draft report was submitted to Treasury for comment in June 1985. In that draft, GAO made a general recommendation concerning the need for verification of the TFCS transactions on which it was seeking the Department's comments. Representatives from our office met with the responsible FMS managers and discussed the strategy that should be used for confirming TFCS transactions shortly after receiving GAO's draft report. We subsequently met with GAO's representatives to discuss the approach we had agreed to with FMS. After some modification, we obtained GAO's tentative concurrence. This plan of action was then offered in the Department's written comments to the draft report. However, as with all of GAO's draft reports, the recipient is cautioned that the draft report does not represent GAO's final position because it is subject to change during their internal review process.

Accordingly, we then waited for the final report to be issued before we would know if GAO formally concurred with the verification approach proposed in response to its recommendation. The final report was issued on September 30, 1985. Afterwards, we worked with FMS in identifying all of the agencies that made payments during the period in question and in preparing the requests for confirmation. The request letters were reviewed and approved by FMS and were mailed by them on January 23, 1986.

We have received no indication from the certifying agencies that the passage of time from when the payments were issued to the time of confirmation has diminished their ability to do a proper verification.

While the confirmation approach being used is a generally accepted auditing procedure, it does not guarantee the legitimacy of the verifications performed by the program agencies. In this regard, we provided copies of the verification request letters to the respective Inspectors General to make them aware of the process and the need for Treasury to be able to periodically confirm transactions.

We have been advised that two audit staffs began reviews of the reconciliation process as a result of our verification activity. The results of these reviews will provide us with very useful information on the current status of agency reconciliation procedures.

APPENDIX 3.—RESPONSES BY WILLIAM E. DOUGLAS, COMMISSIONER, FINANCIAL MANAGEMENT SERVICE, DEPARTMENT OF THE TREASURY, TO ADDITIONAL QUESTIONS SUBMITTED BY THE SUBCOMMITTEE

The following responses for inclusion into the record are to written questions submitted by the Subcommittee on March 17,1986:

Question: In your 1985 Financial Manager's Financial Integrity Act report you stated that all your financial systems are in full conformance with the Comptroller General's principles and standards. However, one of the standards is having an adequate system of internal controls and your report clearly states that the payment systems have significant weaknesses. Therefore, how can your systems be in conformance?

Answer: The FMFIA requires a review of accounting systems (for compliance with Comptroller General principles and standards) and of internal controls for all other operations--in the Financial Management Service this includes payment systems. As far as non-accounting internal controls are concerned, I did not fully assure them. The statement you refer to reads as follows:

> The results of the evaluation, taken as a whole, indicate that the accounting system conforms to the principles, standards, and related requirements of the Comptroller General and with the financial management system objectives of the Office of Management and Budget, except as noted in Enclosure B. Enclosure B describes material instances of nonconformance and shows corrective actions to be taken together with target dates for completion. Enclosure C shows the level of effort expended on the process.

As you can see, there is no inconsistency in my statement.

Question: You stated that you have agreed with all but one of GAO's recommendations and that corrective actions will be completed in fiscal year 1986. What is the current completion date for each recommendation that has not been implemented?

Answer: In my testimony, I stated that we agreed with all but two of the GAO recommendations, have completed nine of them, and the remaining three, which are primarily additional system edits, are in progress.

We intend to complete these last three recommendations before the end of the year.

Question: You did not agree with GAO in the need for a reasonableness edit. However, it is our understanding that in fiscal year 1987 you are going to require agencies to provide a range of payment request numbers that each certifying officer will use for that year. The finance center will then compare the certified payment request number to this "list." Why not request the agencies to also provide a maximum dollar limit for each payment request and compare this "list" to the payment requests received? In addition, GAO's recommendation directed that the agencies would establish the limit and that Treasury could notify the agencies when the limit was too low and thereby causing an unnecessary burden on Treasury. Please provide additional information on why this would be a burden.

Answer: Your question raises the possibility of a "maximum dollar limit for each payment request." In light of the fact that we handle approximately 700 million payments each year, and non-Treasury disbursing offices make an additional 150 million payments, we believe that trying to set up a manual system to monitor such limits would almost certainly lead to "gridlock" and, ultimately, a breakdown of the disbursing systems.

Perhaps your objective might be attained if it was applied on a more limited scale to those payment requests which are most sensitive to possible manipulation or fraud. We would suggest a figure of $100,000 because with that amount at risk you could justify the kind of special procedures which would be required and the volume of effected transactions would still be manageable.

It would be important for GAO to discuss possible changes with program agencies because any meaningful increase in controls in the certification process will primarily impact the program agencies. We do not, of course, want to end up with a "cure" which turns out to be worse than the potential disease.

Question: You stated that no one has improperly used the Treasury Financial Communication System (TFCS) to divert or steal funds. However, we understand that the Secret Service is currently conducting an investigation on a case involving TFCS. Can you comment on this?

Answer: In the case you cited, an authorized official in a non-Treasury program agency prepared a false payment voucher that was reviewed and approved for payment at two levels before it was submitted to Financial Management Service. The documentation of this transaction met all of the requirements for a properly authorized payment.

The key events which led to an improper payment occurred in the program agency during the certification process. Given such circumstances, the payment mechanism involved (in this case, TFCS) is irrelevant.

Question: In your testimony you stated that electronic certification will require the development of a telecommunications network between the 6,000 certifying officers and the 900 locations and Treasury's seven finance centers. It is our understanding that electronic certification can be implemented in a paper-based system using a message authentication code so that a telecommunication network would not be a requirement. Please provide comments on how electronic certification could be implemented in the current system and how much it would cost.

Answer: We know of no way to implement electronic certification in a paper-base system. Any system that uses paper as a medium cannot, by definition, be termed electronic. Electronic certification and message authentication can (and certainly should) be used together in any modern, secure payment system. They are not, however, the same process and do not produce the same results.

Our current system is not capable of supporting either electronic certification or message authentication because of inadequate system capability and capacity and lack of a telecommunication network. We previously furnished the subcommittee with our best estimate of the cost of full-scale implementation.

Question: Does the Treasury directive requiring message authentication apply to agency systems which telecommunicate payment data between their offices? If not, why not?

Answer: Yes.

Question: What is the current status of funding for the testing of message authentication devices? Is the current funding adequate to meet the needs of implementating full electronic certification? If not, why not?

Answer: There are no funds in our FY'86 and FY'87 budgets. With regard to preliminary testing, we have reserved $180,000. We believe a credible pilot, just in the Washington area, would cost at least 10 times that amount.

Prudence dictates such a pilot be undertaken before attempting full-scale implementation across the nation.

Question: On page three of your testimony, you stated that there have been only a few cases of abuse. However, the subcommittee has heard testimony from GAO that the number of abuses and the total dollar loss cannot be ascertained with any degree of certainty because accounting procedures are such that there is no reasonable assurance that fraudulent payments will be detected. Another reason for a lack of comprehensive data cited by GAO is the fact that the responsibility for investigating cases of fraud and abuse rest with a number of agencies. Given the testimony, presented by the Inspector General which documented that a number of unauthorized payments made on a test basis went undetected, do you believe the Treasury/agency reconciliation process identifies all unauthorized payments?

Answer: The Treasury/agency reconciliation process identify all unauthorized payments if the agency follows through on the information provided them. This means that the agency must promptly reconcile the payment data provided them by Treasury.

The IG testimony cited indicates that the agencies do use the reconciliation process in the effective manner except in rare cases.

In addition, agency IGs have been alerted to check the quality and validity of this process during their audits, and we assume that GAO would also be checking agency compliance during its reviews.

Question: Has Treasury or FMS collected any information on abuses to the disbursement systems on a governmentwide basis? If so, please provide the subcommittee with all available data. If not, please comment on the potential usefulness of such an analysis as a means of improving controls over the disbursement systems.

Answer: We have not collected such information about non-Treasury disbursing operations, but we presume that GAO has looked into this matter. If not, we would certainly have no objection to a governmentwide analysis of this area.